REMARKS/ARGUMENTS

The Office Action mailed June 14, 2004 has been reviewed and carefully considered. Claims 2 and 7 are canceled. Claims 1, 3-6, 8-11, 15, and 18 have been amended. Claims 1, 3-6, and 8-18 are pending in this application, with claims 1, 6, and 15 being the only independent claims. Reconsideration of the above-identified application, as herein amended and in view of the following remarks, is respectfully requested.

In the Office Action mailed June 14, 2004, claims 1-11 stand rejected under 35 U.S.C. §103 as unpatentable over U.S. Patent No. 5,812,764 (Heinz) in view of U.S. Patent No. 6,006,333 (Nielsen).

Claims 12-14 and 16-18 stand rejected under 35 U.S.C. §103 as unpatentable over U.S. Patent No. 6,113,078 (Sormunen).

Claim 15 was found to contain allowable subject matter and was indicated as allowable if rewritten in independent form. In view of the allowable subject matter, claim 15 has been rewritten in independent form. Accordingly, it is respectfully submitted that independent claim 15 is now allowable.

Before discussing the cited prior art and the Examiner's rejections of the claims in view of that art, a brief summary of the present invention is appropriate. The present invention relates to a method and an arrangement for remotely accessing password protected services in a data communication system. The present invention is intended for use in systems in which a service provider provides to a user of a service a number of expendable passwords, by means of which a user can access the service via telecommunication and/or data networks (see page 4, lines 12-15 of the specification). The expendable passwords may be single-use passwords (see page 2, lines 14-16). According to the invention, a user's telecommunication device includes a module which

PAGE 9/13 * RCVD AT 9/14/2004 11:34:54 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-50

registers passwords transmitted from a service (page 8, lines 3-13). The module may save passwords for a variety of services (see, e.g., table 1 on page 10). When a user calls a service, the module refers to the list of services and passwords and determines whether the service being called by the user requires a password. If a password is required, the module automatically selects and adds a password to the setup signal or string for transmission to the server (see page 5, lines 1-2; and page 9, lines 14-18). The selected password is then registered as used (page 6, lines 4-6 and page 8, lines 12-13). The server receives the password in the signaling data provided through the telephone network (page 11, lines 1-2).

Independent claims 1 and 6 have each been amended to specifically recite that the password is a single-use password and that the selected password is registered as used when it is selected. Support for these amendments is found in original claims 2 and 7 and at page 2, lines 14-18, page 6, lines 4-6, and page 8, lines 12-13 of the present specification. Independent claims 1 and 6 also recite "selecting from the stored set of single-use passwords, automatically by the terminal device at user log-on to the service, one of the stored passwords for use in logging on to the service" and "transmitting the selected password to the server by adding the selected password to a connection setup signal transmitted from the terminal device to the server via the network to remotely log-on to the service from the terminal device of the user"

Heinz discloses a password management system for passwords used over a communication system. According to Heinz, a server generates a list of passwords which is saved in both the server and the client devices. A client initiates communication from the client device to the server, and the server responds by selecting a password (col. 5, lines 35-39). The server then informs the client of an identifier of the selected password (not the password), and the client then extracts the password from the list at the client device (col. 5, lines 55-59). Since Heinz requires the

PAGE 10/13 * RCVD AT 9/14/2004 11:34:54 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-50

server to select the password in response to the client initiation of communication, Heinz fails to teach or suggest "selecting from the stored set of expendable passwords, automatically by the terminal device at user log-on to the service, one of the stored passwords for use in logging on to the service" and "transmitting the selected password to the server by adding the selected password to a connection setup signal transmitted from the terminal device to the server via the network to remotely log-on to the service from the terminal device of the user", as expressly recited in applicants' independent claims 1 and 6. In contrast to the present invention, Heinz teaches that the client initially sends a connection setup signal without a password. Heinz furthermore teaches that the password is determined by the server and that the client device responds to that selection by the server.

Furthermore, Heinz fails to teach or suggest the use of single-use passwords and registering the selected password as "used" at the terminal device. Instead, Heinz discloses that passwords may be used numerous times in subsequent connections and are changed only when a specified time period has elapsed (see col. 6, lines 30-43 of Heinz). The Examiner refers to col. 6, lines 44-52, of Heinz which states "In the embodiment where passwords are not reused ...". However, Heinz does not mean that the password is a one-time use password. Rather, Heinz allows a password to be used repeatedly for a specific period of time (see page 6, lines 30-31).

Nielsen fails to teach or suggest what Heinz lacks. Nielsen discloses a password helper using a client-side master password which automatically presents the appropriate server-side password to a particular remote server. The master password is used to decrypt a stored password for a particular remote server (col. 1, lines 61-63). Nielsen maintains, at a user operating system 10, a database of passwords and user IDs as they are known to remote sites (col. 3, lines 64-66). The information in the database is encrypted using the master password (col. 3, lines 66-67). When a

PAGE 11/13 * RCVD AT 9/14/2004 11:34:54 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-50

request for authentication is received from a remote site at the user operating system, the appropriate password and ID are decrypted and sent to the remote site (col. 4, lines 1-8). The passwords in the database for the remote sites are not single-use passwords. They are maintained until the user changes them. Furthermore, the master password also stays the same until the user wants to change it. Accordingly, Nielsen fails to teach or suggest that a password is registered as being "used" when it is selected, as recited in independent claims 1 and 6.

Furthermore, since Nielsen discloses that the password is retrieved from the database upon receipt of an authentication request from a remote site, Nielsen also fails to disclose that the password is automatically selected and added to the connection set up signal which is transmitted from the terminal device to the user, as expressly recited in independent claims 1 and 6. In contrast, Nielsen discloses that the terminal first attempts to access the controlled web site and the web site sends an authentication request and the system responds by searching for the correct password (col. 4, line 45 to col. 5, line 3).

In view of the above amendments and remarks, it is respectfully submitted that independent claims 1 and 6 are allowable over Heinz in view of Nielsen.

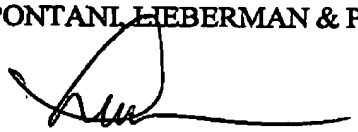
Dependent claims 3-5 and 8-18, each being dependent on one of independent claims 1 and 6, are allowable for at least the same reasons as are independent claims 1 and 6.

PAGE 12/13 * RCVD AT 9/14/2004 11:34:54 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-50

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE



By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: September 14, 2004

PAGE 13/13 * RCVD AT 9/14/2004 11:34:54 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):04-50